QuerySecurityContextToken

A failure of the QuerySecurityContextToken must be detected and handled

Sean Barnum, Cigital, Inc. [vita[1]]

2007-04-02

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 4723 bytes

Attack Category	• Impersonation
Vulnerability Category	• Unchecked Return Value
Software Context	• Authorization
Location	
Description	QuerySecurityContextToken allows a service to impersonate a client. When a service impersonates a client, it acquires an access token (a representation of the client's credentials) from that client and uses it to access resources as if it were the client (impersonate) or check a client's access to resources (identify). For example, if a file server is going to serve files to a client, it should check whether the client has access to these files first. As and example, a Windows file server will do this by getting a client's access token and using it to check against the ACL's of the file being requested. The file server may have permissions to read files that the client does not, or the file server may not have the permissions to read the files that the client can. So in order to secure serve these files, the file server must be able to impersonate the client. A failure of the QuerySecurityContextToken must be detected and handled. The action that would have been performed with the client's access token must not be performed. If it is still performed, it will be performed with the privileges (security context) of the service, not the client. This could result in unauthorized access to sensitive information.
APIs	<table><tr><th>Function Name</th><th>Comments</th></tr><tr><td>QuerySecurityContextToken</td><td></td></tr></table>
Method of Attack	If the return value of this function is not checked, an attacker without the proper authorization to access to the requested resource may still be able to do so simply by requesting the resource. When the request for access fails, the server that called this

[1] http://buildsecurityin.us-cert.gov/bsi/about_us/authors/35-BSI.html (Barnum, Sean)

<table>
<tr><td></td><td>function will continue the routine, using the server's credentials in place of the clients.</td></tr>
<tr><td><b>Exception Criteria</b></td><td>If the return value is properly checked, this function is safe to use.</td></tr>
<tr><td><b>Solutions</b></td><td><table><tr><th>Solution Applicability</th><th>Solution Description</th><th>Solution Efficacy</th></tr><tr><td>This solution is always applicable.</td><td>Check the return value. If it is not SEC_E_OK, don't continue processing the request.</td><td>This solution is always effective.</td></tr></table></td></tr>
<tr><td><b>Signature Details</b></td><td>SECURITY_STATUS SEC_Entry
QuerySecurityContextToken(
PCtxtHandle phContext,
HANDLE* phToken
);</td></tr>
<tr><td><b>Examples of Incorrect Code</b></td><td><pre>/* The return value is not
checked! */
QuerySecurityContextToken(phContext,
phToken);</pre></td></tr>
<tr><td><b>Examples of Corrected Code</b></td><td><pre>/* Fail on error */
if
(QuerySecurityContextToken(phContext,
phToken) != SEC_E_OK)
return -1;</pre></td></tr>
<tr><td><b>Source References</b></td><td><ul><li>MSDN on QuerySecurityContextToken()[2]</li><li>MSDN on Impersonation[3]</li><li>MSDN on Impersonation Levels [4]</li><li>Michael Howard on Impersonation Issues[5]</li><li>Rough Auditing Tool for Security (RATS)[6]</li></ul></td></tr>
<tr><td><b>Recommended Resource</b></td><td></td></tr>
<tr><td><b>Discriminant Set</b></td><td><table><tr><td><b>Operating Systems</b></td><td><ul><li>Windows 2000</li><li>Windows 2003</li></ul></td></tr><tr><td><b>Languages</b></td><td><ul><li>C</li><li>C++</li></ul></td></tr></table></td></tr>
</table>

Cigital, Inc. Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

[1] mailto:copyright@cigital.com